岡山市教育情報セキュリティポリシー

（抜粋版）

平成３１年３月

（令和８年３月改定）

岡山市教育委員会事務局

第１章 教育情報セキュリティ基本方針

１ 目的

岡山市教育情報セキュリティポリシーは，岡山市情報セキュリティポリシーを踏まえつつ，岡山市教育委員会事務局（ただし，教育情報システムの利用や開発，管理等に関することのみ）及び岡山市内の全ての市立学校（小学校，中学校，義務教育学校，高等学校のことをいう。以下，同じ。）が所掌する教育情報資産に係る機密性，完全性及び可用性を維持するための対策の基準を定めることにより，保護者を含む学校関係者等の市民のプライバシー，財産等を保護するとともに，学校業務の適正な運営，並びに教育活動の安全安心な履行に資することを目的とする。

２ 定義

（１）ネットワーク

コンピュータ等を相互に接続するための通信網並びにその構成機器（ハードウェア及びソフトウェア）をいう。

（２）教育ネットワーク

教育委員会事務局が管理するネットワークであり，市立学校において，校務支援システム（自動採点システム，給食会計システム等を含む），インターネット，指導者用及び学習者用端末の利用，並びに学校ホームページの公開等を行うためのネットワークをいう。

（３）外部ネットワーク

インターネットや他部局が管理している行政系ネットワーク（マイナンバー利用事務系，LGWAN 接続系，庁内 LAN 接続系）等，教育委員会事務局が管理していないネットワークの総称をいう。

（４）ウェブサイト

インターネット上に公開された，文字，画像，動画等から成るホームページの集まりをいう。

（５）学校外

市立学校の建物やその敷地以外の場所で，当該学校が管理していない場所をいう。

（６）教育情報

岡山市情報公開条例第２条第２号に規定する「公文書」とともに，教育委員会事務局職員，或いは市立学校の教職員（会計年度任用職員及び臨時的任用職員を含めた教職員全員をいう。以下，同じ。）が職務上作成し，又は取得した文書，図画，写真，フィルム，テープ及び電磁的記録（電子的方式，磁気的方式その他人の知覚によっては認識することができない方式で作成された記録をいう。以下，同じ。）であって，教育委員会事務局の職員及び当該学校の教職員が組織的に用いるものとして，教育委員会事務局及び当該学校が保有しているもの（パブリッククラウド上に保存されているものを含む）をいう。ただし，次に掲げるものを除く。

① 官報，白書，新聞，雑誌，書籍その他不特定多数の者に販売することを目的として発行されるもの

② 図書館その他の施設において一般の利用に供することを目的として管理されているもの

③ 実施機関において歴史的若しくは文化的な資料又は学術研究用の資料として特別の管理がなされているもの

（７）教育情報資産

教育ネットワーク，教育情報システム及び教育情報システムで取り扱う教育情報（印刷された文書を含む），並びに関連設備・機器・電磁記録媒体をいう。

① 教育情報

（ａ）校務系情報

児童生徒の成績，出欠席及びその理由，健康診断結果，指導要録，教員の個人情報など，市立学校が保有する教育情報資産のうち，それらの情報を学校・学級の管理運営，学習指導，生徒指導，生活指導等に活用することを想定しており，かつ，当該情報に児童生徒がアクセスすることが想定されていない情報をいう。

（ｂ）校務外部接続系情報

校務系情報のうち，学校ホームページや教育委員会事務局が調達するクラウドサービスなど，ネットワーク分離による対策を講じたシステム構成において，インターネット接続を前提として，校務で利用される情報をいう。

（ｃ）学習系情報

児童生徒のワークシートや作品など，市立学校が保有する教育情報資産のうち，それらの情報を学校における教育活動において活用することを想定しており，かつ，当該情報に教員及び児童生徒がアクセスすることが想定されている情報をいう。

② 関連設備・機器・電磁記録媒体

（ａ）教育用サーバ（校務系・学習系）

校務系・学習系情報をセグメントで切り分けて取り扱うサーバをいう。

（ｂ）NAS（Network Attached Storage）

ハードディスクとコントローラから構成され，ネットワークに接続して複数の端末でファイルを共有するためのストレージ機器をいう。

（ｃ）校務用端末

校務系情報及び校務外部接続系情報にアクセス可能な端末をいう。

（ｄ）学習者用端末，指導者用端末

学習系情報及び公開系情報の一部にアクセス可能な端末で，児童生徒が利用する端末を「学習者用端末」といい，教員のみが利用可能な端末を「指導者用端末」いう。

（ｅ）庁内 LAN 用端末

行政系ネットワーク（主に庁内 LAN 接続系）にアクセス可能な端末をいう。

（ｆ）電磁記録媒体

USB メモリ，SSD，HDD，CD-ROM 等の電磁的記録を保存するための媒体をいう。

（ｇ）モバイル Wi-Fi ルータ，ホームルータ

携帯電話回線(4GLTE 等の回線)を利用することで外部ネットワークに接続する通信機器のうち，持ち運び型をモバイル Wi-Fi ルータ，据え置き型をホームルータという。

③ 教育ネットワーク

（ａ）校務系ネットワーク

教育用サーバ（校務系）と校務用端末の通信及びインターネット接続を取り扱うネットワークをいう。

（ｂ）校務外部接続系ネットワーク

ネットワーク分離による対策を講じたシステム構成において、校務外部接続用端末から校務外部接続系システムやクラウドサービス等との通信を取り扱うネットワークをいう。

（ｃ）学習系ネットワーク

教育用サーバ（学習系）と学習者用・指導者用端末の通信及びインターネット接続を取り扱うネットワークをいう。

④ 教育情報システム

以下に示す，校務系システム，校務外部接続系システム及び学習系システムを合わせた総称をいう。

（ａ）校務系システム

校務系ネットワーク，校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステムであり，当該情報を扱う上で，適切なアクセス権が設定された領域で利用されるシステムをいう。

（ｂ）校務外部接続系システム

校務外部接続系ネットワーク，メールサーバ，ホームページ運用サーバ等から構成される校務外部接続系情報を取り扱うシステムをいう。

（ｃ）学習系システム

学習系ネットワーク，学習系サーバ，学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステムであり，当該情報を扱う上で，適切なアクセス権が設定された領域で利用されるシステムをいう。

（８）情報セキュリティ，情報セキュリティインシデント

① 情報セキュリティ

教育情報資産について，以下に示す機密性，完全性及び可用性を維持することをいう。

（ａ）機密性

情報にアクセスすることを認められた者だけが，情報にアクセスできる状態を確保することをいう。

（ｂ）完全性

情報が破壊，改ざん又は消去されていない状態を確保することをいう。

（ｃ）可用性

情報にアクセスすることを認められた者が，必要なときに中断されることなく，情報にアクセスできる状態を確保することをいう。

② 情報セキュリティインシデント

本編第３項「対象とする脅威」の①～⑤に示すような，不正アクセスや不正使用，人為的ミス，自然災害等の脅威により発生する事件・事故のことをいう。

（９）本市の管理体制及び責任者等

① 最高情報セキュリティ責任者（CISO：Chief Information Security Officer）

副市長（政策局担当）をもって充て，本市における全ての情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

② 最高情報セキュリティ責任者補佐監（CISO 補佐監）

政策局政策部デジタル担当部長をもって充て，CISO を補佐するとともに，全てのネットワークにおける開発，設定の変更，運用，見直し，情報セキュリティ対策等に関する権限及び責任を有する。

③ 全庁ネットワーク管理者

政策局政策部デジタル推進課情報システム担当課長をもって充て，情報システム管理のうち，庁内 LAN の運用管理の統括及び総合調整を行う。

④ 情報セキュリティ推進本部

「岡山市情報セキュリティ推進本部設置規程」第１条に基づき，情報セキュリティ対策を組織的かつ継続的に推進していくために設置する組織をいう。

⑤ 情報セキュリティインシデント統括窓口（CSIRT）

情報セキュリティインシデントに関する統一的な窓口として，CISO 補佐監の下に置かれる組織をいう。

⑥ 岡山市情報セキュリティポリシー（平成 25 年６月策定，令和７年 10 月改定）
市長その他の執行機関，その他法律の規定に基づき本市に置かれる機関を適用範囲とし，本市が所掌する情報資産について，セキュリティの脅威から機密性，完全性及び可用性を維持するための対策の基準等をいう。

⑦ 岡山市教育情報セキュリティポリシー
基本方針編（第１章），対策基準編（第２章），実施手順編（第３章）で構成する本冊のことをいう。岡山市情報セキュリティポリシーの改定状況等を踏まえて改定を行う。

⑧ 教育委員会事務局及び市立学校の組織体制
岡山市教育情報セキュリティポリシー対策基準編及び実施手順編に明示する。

３ 対象とする脅威

教育情報資産に対する脅威として，以下①～⑤の脅威を想定し，情報セキュリティインシデントを未然に防ぐための情報セキュリティ対策を実施する。

① サイバー攻撃をはじめとする部外者の侵入，不正アクセス，ウイルス攻撃，サービス不能攻撃，内部不正等の意図的な要因による教育情報資産の漏えい・破壊・改ざん・消去，重要情報の詐取，サービス停止等
② 無許可のハードウェア，ソフトウェアの使用等の規定違反，設計・開発の不備，プログラム上の欠陥，操作・設定ミス，メンテナンス不備，監査機能の不備，委託管理の不備，マネジメントの欠陥，機器故障等の偶発的要因による教育情報資産の漏えい・破壊・消去等
③ 地震，水害，落雷，火災等の災害によるサービス及び業務の停止等
④ 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
⑤ 電力供給の途絶，通信の途絶等のインフラの障害からの波及等

４ 適用範囲

（１）行政機関等の範囲
本章が適用される範囲は，教育委員会事務局（ただし，教育情報システムの利用や開発，管理等に関することのみ），教育委員会（教育情報資産を扱う場合のみ）及び市立学校とする。

（２）教育情報資産の範囲
本基本方針が対象とする教育情報資産は，次のとおりとする。

① 教育ネットワーク，教育情報システム，これらに関する設備，電磁的記録媒体
② 教育ネットワーク及び教育情報システムで取り扱う情報（これらを印刷した文書を含む。）
③ 教育情報システムの仕様書及びネットワーク図等のシステム関連文書

（３）適用対象外
行政系ネットワークで管理する教育情報システムは，（１）及び（２）に定める適用範囲から除き，岡山市情報セキュリティポリシーを適用する。

（４）定めのない場合
本基本方針に定めのない場合は，岡山市情報セキュリティポリシーの該当部分を準用するものとする。

５ 教職員の遵守義務

教職員は，情報セキュリティの重要性について共通の認識をもち，業務の遂行に当たって教育情報セキュリティポリシーを遵守しなければならない。

６ 情報セキュリティ対策

本編第３項「対象とする脅威」の①～⑤の脅威から教育情報資産を保護するために，以下の情報セキュリティ対策を講じる。

（１）組織体制

市立学校の教育情報資産について，情報セキュリティ対策を推進する組織体制を教育委員会事務局及び市立学校ともに確立する。

（２）教育情報資産の分類と管理

市立学校の保有する教育情報資産について，機密性，完全性及び可用性の三つの観点から影響度を評価して以下の４段階の分類を行い，当該分類に基づき情報セキュリティ対策を行う。

（３）物理的セキュリティ

サーバ，情報システム，通信回線，LAN ケーブル及び教職員・児童生徒が利用するパソコン等の端末並びに教育情報資産を取り扱うその他の設備及び機器の管理について，物理的な対策を講じる。

（４）人的セキュリティ

情報セキュリティに関し，教職員が遵守すべき事項を定めるとともに，児童生徒を含めた十分な教育及び啓発を行う等の人的な対策を講じる。

（５）技術的セキュリティ

コンピュータ等の管理，アクセス制御，システムの開発・導入・保守，不正プログラム対策，不正アクセス対策等への技術的対策を講じる。

特に，インターネットを通信経路とする前提で，内部・外部からの不正アクセスを防御できるよう，利用者認証（多要素認証），端末認証，アクセス経路の監視・制御等を組み合わせた強固なアクセス制御を行う。

（６）運用

情報システムの監視，教育情報セキュリティポリシーの遵守状況の確認，業務委託を行う際のセキュリティ確保等，教育情報セキュリティポリシーの運用面の対策を講じるものとする。また，情報セキュリティインシデントが発生した場合等に迅速かつ適切に対応するため，緊急時対応手順を策定する。

（７）業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合，委託事業者を選定し，情報セキュリティ要件を明記した契約を締結し，委託事業者において必要なセキュリティ対策が確保されていることを確認し，必要に応じて契約に基づき措置を講じる。

約款による外部サービス（クラウドサービス）を利用する場合には，利用にかかる規定を整備し，対策を講じる。

ソーシャルメディアサービスを利用する場合には，ソーシャルメディアサービスの運用手順を定めるとともに，ソーシャルメディアサービスで発信できる情報を規定し，利用するソーシャルメディアサービスアカウントごとの責任者を定める。

７ 情報セキュリティ監査及び自己点検の実施

教育委員会事務局は，教育情報セキュリティポリシーの遵守状況を検証するため，定期的又は必要に応じて市立学校に対して教育情報セキュリティ監査を実施する。監査は，委託事業者による監査又は職員による内部監査を適宜選択して実施しなければならない。

また，市立学校は，定期的又は必要に応じて，監査結果等を踏まえた自己点検を実施する。

８ 教育情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検等の結果，教育情報セキュリティポリシーの見直しが必要となった場合，又は情報セキュリティに関する状況の変化に対応するため新たに対策が必要となった場合には，保有する教育情報及び利用する教育情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し，リスクを検討したうえで，教育情報セキュリティポリシーを見直す。

９ 教育情報セキュリティ対策基準の策定（本表第２章が該当）

上記６，７及び８に規定する対策等を実施するために，具体的な遵守事項及び判断基準等を定める「教育情報セキュリティ対策基準」を策定する。

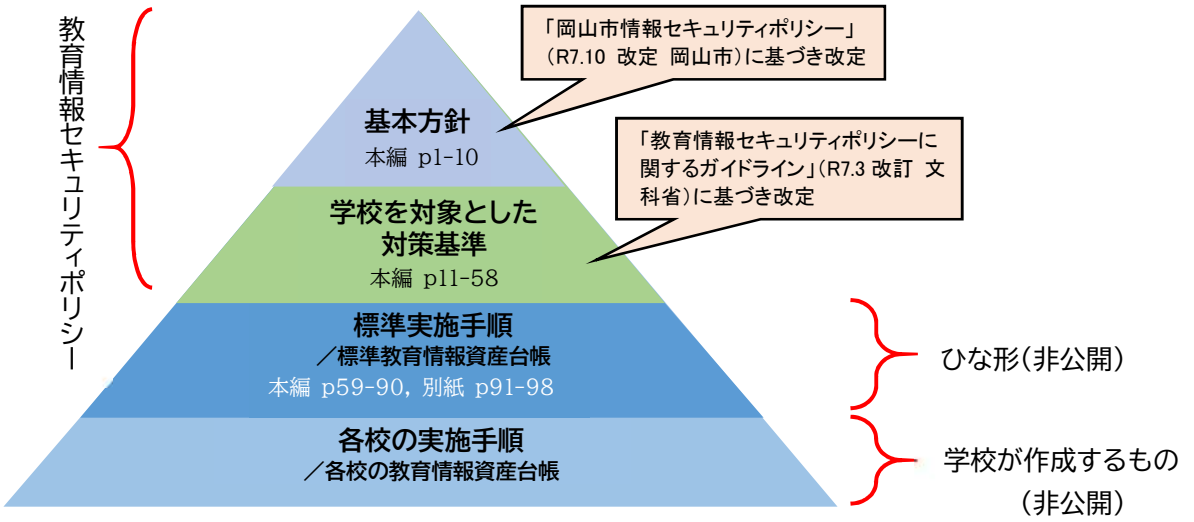
10 教育情報セキュリティ実施手順の策定（本表第３章が該当）

情報セキュリティに関する対策の具体的な実施手順は，教育情報セキュリティポリシーで定める教育情報セキュリティ対策基準に基づき，学校共通の実施手順として策定し，必要に応じて見直しを行うものとする。

また，各学校においては，教育委員会が示す「標準実施手順」を踏まえて，各校の実態に応じた実施手順を作成しなければならない。

なお，教育情報セキュリティ実施手順は，公にすることにより情報セキュリティインシデントを誘発する可能性があり，また，業務等に重大な支障を及ぼすおそれがあることから当該実施手順は非公開とする。

【教育情報セキュリティポリシーの体系図】



附則

この基本方針は，平成３１年３月１日から施行する。
この基本方針は，令和３年２月１日から施行する。
この基本方針は，令和７年２月 18 日から施行する。
この基本方針は，令和８年３月１日から施行する。